

Security Awareness

March 2003

New Enterprise Policy	Bad Passwords are Bad News	Cyber Bytes
Homeland Security	Securing Your Workstation	Microsoft Information
Importance of Applying Security Patches	Email Impersonators	Useful URLs

Foreword

In an effort to emphasize the importance of information security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide the Security Awareness Newsletters. It is hoped these newsletters will be a valuable resource, providing practical tips, security solutions, and job-saving techniques.

Also, as a friendly reminder, GOT staff are encouraged to familiarize themselves with all security policies, manuals, and procedures which can be found at [GOT Policies and Procedures](#).

[Back to Top](#)

New Enterprise Policy on Computer Sanitization



The Governor's Office for Technology (GOT) has recently released an enterprise policy for the sanitization of information technology equipment and electronic media. The policy provides recommended guidelines for cleaning computer hard drives and other electronic media of sensitive/confidential data when preparing for surplus or disposal.

Some may have the impression that simply deleting files from a hard drive or using the Format or FDISK command will permanently delete data; however, with the proper knowledge and tools, data can still be recovered unless the drive is properly sanitized. GOT recommends that agencies use a disk cleaning utility software such as WipeDrive or SecureClean that conforms to the US Department of Defense's requirements for disk sanitization (5220.22-M). For more information, please review the [enterprise policy](#).

[Back to Top](#)

GOT Homeland Security Advisory Alert Plan



With the recent elevation of the national homeland security threat level to orange (indicating a possible high threat of terrorist attacks), the Governor's Office for Technology (GOT) has enacted its own alert plan to enhance security at its mission critical computing facilities. Following 9/11, GOT began preparing its Homeland Security Advisory Alert Plan, which details implementation procedures for GOT organizations to initiate for each threat level. During the Orange threat level, GOT will continue to closely scrutinize the physical security of its facilities. As a result, the Commonwealth Data Center (CDC) has been closed to visitors and non-essential personnel for the duration of the alert and the visitor parking areas at the CDC have been restricted to traffic. GOT will also continue to carefully monitor security alerts and reports of security-related incidents. GOT strongly recommends that all state agencies also devise a plan to protect critical information technology

resources and infrastructure.

If you're interested in learning more about homeland security, check out the [Kentucky Homeland Security](#) website or the [US Department of Homeland Security](#) site.

[Back to Top](#)

The Importance of Applying Security Patches

In January of this year, the Internet was crippled by a worm that took advantage of a vulnerability in the Microsoft SQL Server software, causing denial of service (DoS) attacks that affected over 75,000 vulnerable hosts. The Sapphire/Slammer worm jammed networks throughout the world, including the Kentucky Information Highway (KIH) -- the statewide infrastructure that provides network and communications services to state government, as well as many cities, counties, schools, libraries and others across the state. Experts estimate that it took the worm only 10 minutes to spread worldwide. Amazing, you say, that something could spread so fast and affect so many! What is truly amazing is that this attack could have been prevented or, at least, its severity lessened by installing a single patch from Microsoft that was available six months earlier in July 2002. GOT urges all agencies to implement procedures to ensure security patches/updates are installed on a timely basis. GOT's Division of Security Services provides up-to-date information on hardware/software vulnerabilities and malicious



code at its Security Alert [website](#). Fortunately, the Sapphire/Slammer worm caused minimal damage. The next attack might not be as benign.

[Back to Top](#)

Bad Passwords are Bad News!



In early March, 2003, the Internet experienced a spike in Internet traffic caused by the Deloder worm -- a worm that exploited a common vulnerability today in computer security -- BAD PASSWORDS! According to CNET News, the worm may have affected over 10,000 computers using a list of 86 passwords to break into computers running Microsoft Windows NT, 2000 and XP. The first line of defense in a secure system is a strong password.

GOT recommends that passwords be at least 8 characters in length and contain upper and lower case letters and numbers. The use of a special characters are also highly recommended because they make it harder for attackers to crack your password. Also note that passwords should never be shared or written down. By doing something as simple as creating a complex password, you can protect your computer from intruders and threats such as the Deloder worm. More information on Deloder can be found [here](#).

[Back to Top](#)

Securing Your Workstation when You're Away

Imagine this... your 10:00 meeting is about to start but you still need to make 20 copies of the financial report. You leave your office in a rush without locking your workstation or activating the password protected screensaver. When you get out of your meeting, you find that the report you've spent 2 weeks working on has been deleted and someone has sent an unflattering email to your boss from your email account. Sounds like an unlikely scenario but it can and does happen, especially if you leave your workstation open to anyone when you're away from your office. Not only does not securing your workstation endanger your files and data, it can also open up the network to possible attacks, divulging sensitive/confidential information and/or causing a major disruption to systems.



One way to protect your computer from unauthorized access is to lock it by pressing CTRL+ALT+DEL on your keyboard and then selecting Lock Computer. Another way to secure your computer is to activate a password-protected screensaver when you're away. This can be done in most Windows based systems by selecting the Display Icon in the Control Panel and clicking on the Screensaver tab. Be sure to check the Password Protected box to require authentication before allowing access. GOT also recommends that users completely power down (turn off) their machines at night--not just the monitor--but the CPU box also.

[Back to Top](#)

Don't Trust that Email! -- Email Impersonators



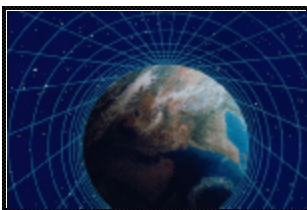
★ There seems to be a lot of impersonators out there these days and we're not talking about entertainers mocking your favorite celebrity. Many people have reported receiving email from seemingly reputable sources such as AOL, Earthlink and other internet service providers requesting users to cough up information on their passwords and credit card numbers. One email went as far as to ask for the person's mother's maiden name, driver's license and social security numbers!

★ Other impersonator incidents include the posting of false jobs on boards like monster.com just to steal personal data from job applicants. According to CNet News, "Identity theft has been a growing problem, both online and offline. Earlier this year, the Federal Trade Commission said ID theft complaints rose 73 percent from the previous year."

If you receive an email asking you to divulge personal information such as password or credit card information, even though it may look authentic, **DON'T DO IT!** You're exposing yourself to possible identity theft. If you do receive an email requesting sensitive information, contact the company by telephone to verify the request and then provide the information via the phone. For more information on email impersonators, click [here](#). To find out more information on false job postings, click [here](#).

[Back to Top](#)

Cyber Bytes



Girl's Email Experiment Clogs Inbox for Weeks

15 year old Shannon Syfrett, emailed 63 people as part of a school project to find out how far a chain mail would go. Ironically, she used a new AOL account to 'spread the word'. At the end of it, Shannon received 160,478 responses from 189 countries!! For more, click [here](#).

Note: Forwarding or responding to emails such as Shannon's is not appropriate and against the [Commonwealth's Enterprise Internet and Email Acceptable Use policy](#).

Companies Throw Security Out with the Garbage

Identity theft is now the largest form of white-collar crime in the western world, but not because the Internet has made it easier to steal personal information. For more, click [here](#).

[Back to Top](#)

Microsoft Information

Unchecked Buffer in Windows Component Could Cause Web Server Compromise (815021)

Microsoft Windows 2000 supports the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. WebDAV is a set of extensions to the Hyper Text Transfer Protocol (HTTP) that provide a standard for editing and file management between computers on the Internet. A security vulnerability is present in a Windows component used by WebDAV, and results because the component contains an unchecked buffer.

An attacker could exploit the vulnerability by sending a specially formed HTTP request to a machine running Internet Information Server (IIS). The request could cause the server to fail or to execute code of the attacker's choice. The code would run in the security context of the IIS service (which, by default, runs in the LocalSystem context).

Although Microsoft has supplied a patch for this vulnerability and recommends customers install the patch immediately, additional tools and preventive measures have been provided that customers can use to block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch. Click [here](#) for patch. For more detailed information on this bulletin, click [here](#).

Unchecked Buffer in Windows Redirector Could Allow Privilege Elevation (810577)

The Windows Redirector is used by a Windows client to access files, whether local or remote, regardless of the underlying network protocols in use. For example, the "Add a Network Place" Wizard or the NET USE command can be used to map a network share as a local drive, and the Windows Redirector will handle the routing of information to and from the network share.

A security vulnerability exists in the implementation of the Windows Redirector on Windows XP because an unchecked buffer is used to receive parameter information. By providing malformed data to the Windows Redirector, an attacker could cause the system to fail, or if the data was crafted in a particular way, could run code of the attacker's choice. For more detailed information on this bulletin, click [here](#).

Cumulative Patch for Internet Explorer (810847)

Subsequent to the initial release of this bulletin, a non-security issue was discovered with the IE 6 version of this patch that could affect some users - primarily consumers - under certain conditions. Specifically, the issue could cause some IE 6 users to be unable to authenticate to certain Internet websites such as subscription based sites, or MSN email. This issue has been resolved, and a hot fix ([813951](#)) issued to correct it. It is important to note that this hot fix corrects a very specific non-security issue in IE 6 only, and that the security patch discussed in this Security Bulletin was, and still is, effective in removing the vulnerabilities discussed later in this bulletin. More information, including details of how to obtain the hot fix are available at: <http://www.microsoft.com/windows/ie/downloads/critical/813951/default.asp>

[Back to Top](#)

Useful URLs

www.cert.org

The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com

Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com

Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through email, voice message, fax, or SMS (Small Message Service) on wireless phones. SIA provides all known information available about vulnerabilities, their causes, and severities creating actionable information to bolster computers from attack.

<http://www.zdnet.com/>

ZDNet operates a worldwide network of websites for people who want to buy, use, and learn about technology. Winner of the Computer Press Association's "Best Overall Site" award for two consecutive years, ZDNet provides an invaluable perspective and resources for technology decision makers to gain an edge in business.

<http://www.searchsecurity.com/>

SearchSecurity.com is the home of TechTarget, offering the most targeted media for enterprise IT professionals, including industry-specific websites, more than 100 email newsletter titles, print media, exclusive, invitation-only conferences, live online events and list rentals.

[Back to Top](#)

Sources: ZDNet, Yahoo, PCWorld, MSN.com, Microsoft.com, CNet News.com